IN THE UNITED STATES DISTRICT COURT

IN AND FOR THE DISTRICT OF DELAWARE

- - -

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	:	CIVIL ACTION
	:	NO. 12-MD-2358 (SLR)

- - -

Wilmington, Delaware
Thursday, July 25, 2013
2:00 o'clock, p.m.

- - -

BEFORE: HONORABLE SUE L. ROBINSON, U.S.D.C.J.

- - -

APPEARANCES:

KEEFE BARTELS, LLC
BY: STEPHEN G. GRYGIEL, ESQ.
(Red Bank, New Jersey)

-and-

STRANGE & CARPENTER
BY: BRIAN RUSSELL STRANGE, ESQ.
(Los Angeles, California)

-and-

Valerie J. Gunning
Official Court Reporter

APPEARANCES (Continued):

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.
BY: JAMES P. FRICKLETON, ESQ. and
EDWARD D. ROBERTSON, JR., ESQ.
(Leawood, Kansas)

-and-

FINGER & SLANINA, LLC
BY: DAVID L. FINGER, ESQ.

Counsel for Plaintiffs

FISH & RICHARDSON, P.C.
BY: SUSAN M. COLETTI, ESQ.

-and-

SIDLEY & AUSTIN LLP
BY: ALAN CHARLES RAUL, ESQ.
(Washington, D.C.)

Counsel for Defendant
PointRoll Inc.

WILSON SONSINI GOODRICH & ROSATI
BY: MICHAEL H. RUBIN, ESQ. and
ANTHONY J. WEIBELL, ESQ.
(Palo Alto, California)

Counsel for Defendant
Google

APPEARANCES (Continued):

MORRIS, NICHOLS, ARSHT & TUNNELL
BY: RODGER D. SMITH, II, ESQ.

-and-

ROPES & GRAY LLP
BY: DOUGLAS H. MEAL, ESQ. and
LISA M. COYLE, ESQ.

Counsel for Defendants
Media Innovation Group, LLC and WPP plc

RICHARDS, LAYTON & FINGER, PA
BY: RUDOLF KOCH, ESQ.

-and-

VENABLE LLP
BY: EDWARD P. BOYLE, ESQ. and
DAVID CINOTTI, ESQ.
(New York, New York)

Counsel for Defendant
Vibrant Media Inc.

- - -

P R O C E E D I N G S

(Proceedings commenced in the courtroom, beginning at 2:00 p.m.)

THE COURT: All right. Let's start out with introductions, if we could. Let's start with plaintiffs' counsel.

MR. STRANGE: Good afternoon, your Honor. Brian Strange for the plaintiff class.

THE COURT: All right. Thank you.

MR. ROBERTSON: Your Honor, Edward Robertson for the plaintiff class.

MR. GRYGIEL: Good afternoon, your Honor. Steve Grygiel for the plaintiffs.

MR. FRICKLETON: And James Frickleton for the plaintiffs.

THE COURT: All right. Thank you.

MR. FINGER: Good afternoon, your Honor. David Finger for the plaintiffs.

THE COURT: All right. Start with one of the defendants.

MR. RUBIN: Good afternoon, your Honor. Michael Rubin of Wilson Sonsini for defendant Google.

MR. WEIBEL: Anthony Weibel for defendant

Google.

MR. MEAL: Douglas Meal for defendants WPP and Media Innovation Group.

MR. SMITH: Good afternoon, your Honor. Rodger Smith from Morris Nichols, for the same two defendants, WPP and Media innovation.

MR. KOCH: Rudy Koch from Richards, Layton & Finger on behalf of Vibrant Media, Inc.

MR. CINOTTI: Davidson Cinotti for the defendant Vibrant.

MR. BOYLE: Good afternoon, your Honor. Edward Boyle for defendant Vibrant.

MS. COLETTI: Your Honor, Susan Coletti from Fish & Richardson for PointRoll.

THE COURT: All right. Thank you.

MR. RAUL: Alan Raul, also for PointRoll.

MR. NICHOLS: Brent Nichols, Sidley & Austin, for PointRoll.

THE COURT: All right. Thank you very much.

These, I believe, we're hearing argument on defendants' motion. Have you coordinated your argument so I'm not hearing the same thing four times, three times?

MR. RUBIN: Indeed, we have.

THE COURT: All right. You may proceed.

MR. RUBIN: Good afternoon again, your Honor.

Michael Rubin of Wilson Sonsini for defendant Google.

On the point of coordination, I'm going to present argument for all three remaining defendants. I believe you saw yesterday that PointRoll had settled with the plaintiffs. There may be an issue here or there where the parties differ. If your Honor has questions, counsel for one of the other defendants can rise and address those.

THE COURT: All right.

MR. RUBIN: But at this stage, we all believe that common issues running through all of, in effect, all of the defendants can be resolved right now and a favorable ruling on a motion to dismiss.

THE COURT: All right.

MR. RUBIN: So this case has seen a fair bit of complexity. There are a lot of lawyers here today. I remember the last time I was here, it was a fairly chaotic day.

The issues in Google's motions to dismiss are quite straightforward. Plaintiffs allege that they were users of apples Safari web browser and Microsoft's Internet web browsers. Notably, that they used those browsers in their default settings exactly how they came from Apple and Microsoft, and that Google and the other defendants set cookies on those browsers. Also notably, they don't actually allege that any of the defendants had cookies on

their browsers, just that cookies were set on browsers generally.

Our motion is straightforward because two issues decide, and those two issues run through each of the claims and plaintiffs' claims to standing here, and those two issues are pleaded clearly within the four corners of the complaint.

Together, they can decide the case in Google's favor, and they're these two issues. Plaintiffs do not and cannot allege causation, and they do not and cannot allege harm. And those two fundamental facts are enough to allow this Court to dismiss the complaint as is routinely done in cases like this.

We've cited a litany of cases in our papers and I'm happy to walk through some of them today, if it would be helpful, but this is not a unique posture for a case like this, alleging these types of claims, certainly over cookies. This has been the history for a decade. Cases like this are broad and on motions to dismiss. Particularly where plaintiffs have been unable to articulate harm, the courts dismiss them.

I'd like to walk through quickly the two salient points that resolve through all the claims, and I will walk through most of them, skipping where I can to save some time. But I think I also commend your Honor to

review the briefs where all of this is laid out in great detail.

THE COURT: Yes.

MR. RUBIN: And I can see from your face that you know that sometimes it's laid out by multiple parties. So you'll forgive me if I'm in some places brief and refer you to the briefs.

The first issue is this. Plaintiffs argue that Google and the other defendants used cookies to collect information about them, but the consolidated complaint makes absolutely clear that the information they're upset was collected is actually sent by plaintiffs' browsers directly to the services.

And I'm going to get back to it for a second because I think it's quite important here to parse out the communications at issue, what's being sent.

If we look at -- a few relevant paragraphs of the complaint. I will point them out as I'm going.

Plaintiffs really allege a few independent communications, only one of them that actually goes to the defendant. They allege that they type URLs into browsers. URLs are a uniform brief. That's indicated in the browser like CNN.com.

Plaintiffs say that -- these are what are called get requests. The technical term for how that's sent

is a get request. It's the HTML. Hypertext market language.

They allege, and this is true, it's a factual allegation and it happens to be actually descriptive of how the Internet works. They allege that that get request contained some information about the browsers, what we've referred to as browser-generated information, so that we didn't have to constantly refer to this litany of things in the briefs.

But the things include IP address, the type of browser they're using, the screen resolution and, importantly, the URL contains that information. Otherwise, they wouldn't be able to get to where they're going.

They allege two other communications happened if the defendants are involved. If the website wishes to display, for example, a Google ad, the website sends an instruction back to the browser, telling the browser, browser, send all that information you just sent me to Google, or in this case technically it would be double click, but send that over there so that they can send me the right ad to populate into your browser and then all of that same information, all of that browser-generated information, is set in another get request, not to the website this time, but directly from the browser to the service, in this case, to Google. That's a direct transmission, direct

communication.

And cookies played no part in this. Cookies don't enable that communication. That communication occurs on browsers that don't have any cookies. It would have occurred on their browsers long before they ever got a cookie. If they actually did get a cookie, it would occur on them afterwards. Cookies simply play no role in this. And the same information is sent with a cookie as without a cookie.

But plaintiffs' case is directed in large part to how Google and the other defendant placed users, rather, placed cookies on users browsers. Plaintiffs say -- these are a lot of words, but they say that defendants tricked their browsers. But, in fact, the functionality that was used to place these cookies was functionality that was designed into the browsers by Apple and Microsoft. But at the end of the day, particularly for this motion, that's entirely besides the point, because the information that plaintiffs argue Google and the other defendants shouldn't have been receiving, they would have been receiving anyway without these cookies, as I just explained. These get requests come anyway.

And plaintiffs had been sending it, that information to Google and defendants and countless others, not just these defendants -- that's the way browsers work --

long before this case arose and they'll be sending it long before this case gets resolved, because that's just how the Internet works.

And that explains why they can't allege a credible theory of harm for the jury, which brings me to my second point, the one that resolves this point. They have not alleged they've suffered any cognizable harm. Really, in paragraphs 242 to 244 of their complaint, way back, interestingly, in a cause of action that's directed only to Google, they assert that they lost the opportunity to sell their information at full value. This sort of diminished value theory has been consistently rejected by courts.

And putting aside that Google would have received the information with or without the cookies, plaintiffs allege no facts that would allow the Court to infer that they ever tried to sell their information, that they ever had an opportunity to sell their information, let alone how or why the conduct that they allege here undermine their ability to sell it and reduce the value for which they were offered it. And this lack of causation and harm to the named plaintiffs, because the harm has to be to one of these four named plaintiffs, requires dismissal of the complaint.

First, I am going to address standing. Then I'm

going to walk through some of the key causes of action.

Plaintiffs select standing for two basic reasons. First, they have not alleged harm, as I just explained. I'm going to walk through that a bit more. And they have not alleged sufficiently the elements of the statutes and they can't allege the elements of the statutes that they say excuse their inability to allege harm.

Fundamentally, it's simply not enough to allege that your information has been tracked or accessed. You have to allege some resulting harm from that access or track, and plaintiffs have not and cannot do that.

So as I mentioned, plaintiffs claimed to have lost the opportunity to sell their personal information at full value, but there are no facts whatsoever in the complaint that support that allegation, and therefore it's merely a conclusion that the Court can't credit.

What they do instead, because they're unable to allege facts about themselves, is they cite studies and services that had no connection to them or to this case. None of them involved the consumer receiving payment for the sort of information that's involved here, the information that a browser sends a get request that they allege is in their complaint.

They all involve either academics postulating

about the intrinsic value of personal information or some services that allow people to pay to have certain information protected. There's nothing akin to what's at issue here.

Ultimately, they simply have not shown that they suffered injury in fact, let alone, let alone when it's concrete and particularized and not conjecture and certainly one that's not traceable to them.

A long line of cases have dismissed privacy claims on the very same grounds. These are in our briefs, but I will mention them briefly. The LaCourt versus Specific Media case, DelVecchio v. Amazon, and very recently, the younger versus Pandora Media case.

Also, in re Google Privacy Policy Litigation, Lowe versus LinkedIn and Jet Blue. This is a line that goes back very long.

In the end, plaintiffs say, though, that they actually don't need to allege that kind of harm. They don't need to allege it because they've asserted some statutes here and that the statutes provide that standing.

Plaintiffs appear to misunderstand the rule. Merely reciting the elements of a statute is not enough to invoke the standing that the standing might confer. The elements of the statute must be plausibly met and they certainly can't be contradicted by the allegations, as they

are here. The fact that they're contradicted means that plaintiffs can't rely on a statutory standing basis to -- as a basis for proceeding with their litigation.

And notably, there's only, only one set of claims that even contain a statutory standing possibility, and that's those under the Wiretap Act. The rest of the claims, even those that are based on statutes, expressly require some sort of injury.

For example, the Federal Computer Fraud and Abuse Act has a statutory standing requirement far higher than Article III standing, and I will get to that in a moment, and some of the California statutory claims also have standing requirements far above Article III, and if they can't meet Article III, they certainly can't meet those statutory requirements.

So looking at the Wiretap Act, where plaintiffs say they don't need to allege harm, the Wiretap Act itself says I get damages if the provisions are violated.

Plaintiffs need to show that the provisions are violated and they can't. So the federal claims that they assert simply don't fit here. The Wiretap Act and the Source Communications Act simply don't fit, not to mention the remarkable tension between asserting those two claims.

So the very first step you need to take when you are looking at a Wiretap Act claim is to look at what the

communication is, because otherwise you can't analyze as a fact-finder what's going on. You can't look, you can't try to make a decision.

Here, we don't have to question that. The complaint very clearly in its early stages, in paragraphs between 30 and 45, very clearly explain, I think it's paragraph 41 that does the most work on this, that it's the get request that I explained earlier.

The get request from plaintiffs' browsers to defendants in response to the website that they visit, that is the communication that defendants receive. They don't receive anything else. Defendants can't possibly be a party to a communications that goes directly from plaintiffs' browsers to another website. It's simply not how the Internet works.

And so in light of that, there are two reasons why the Wiretap Act claim can't proceed, because the elements aren't met. The first and perhaps the simplest is because Google is a party to the communication, and the Wiretap Act is somewhat of a strange beast. It sets out a broad prohibition against interception and then carves out a very significant number of exceptions to that. So seeking an exception to the Wiretap Act is nothing abnormal. It happens all the time.

When we receives e-mails, when your Honor

receives e-mails, those are interceptions of electronic communications, but we're intended recipients of them. We're parties to them, so they're not violations of the Wiretap Act. All sorts of things we do in our daily life are excused from liability under the Wiretap Act because we're parties to those communications. The same here. Material that is sent directly to a party can't be subject to a Wiretap Act claim. But even if we credited a claim and even if you could imagine a world in which the communication prior to the placement of the cookie was sent and then the cookie was placed and then the next day it was the same type of communication, but there was a cookie there and you looked past the party exception, kind of hard to do that, but if you look past the party exception, you can't get past the other requirement of the Wiretap Act, which is that it only covers the interception of contents, and that is something related to the substance, report or meaning of the underlying communication.

And as plaintiffs' complaints make clear, these cookie values are just strings of text, a bunch of different characters. They don't change based on what is in the web page that's being sent. They're not related to the substance or meaning of that page. The cookie value does not tell you what's on the website. It's not content. It's transactional information, at most, and transactional

information has been routinely held to be outside the scope of the Wiretap Act. The senders of an e-mail, the who, what, where, when and why, that's all outside the Wiretap Act. The Wiretap Act protects communication and that's simply not anything that they've asserted here. So the Wiretap Act cannot provide plaintiffs with a basis for having standing.

There's another claim that plaintiffs have asserted similar to the Wiretap Act. It's actually its mirror opposite and its the claim under the Stored Communications Act. It's Count 2.

I first have to just point out that the exact same alleged facts cannot support both a Wiretap Act claim and a stored communications claim. They're mutually exclusive. And while I'm going to go a little bit further on this, I don't think we need to go much further than looking at the allegations that plaintiffs make that these communications were intercepted in transit. They make this in their attempt to make the square pegs of their facts fit the round hole of the Wiretap Act. They go to great length to articulate how these communications were intercepted in transit.

The Stored Communications Act only applies to communications that are accessed well in a certain limited type of electronic storage, where that storage is being done

by a certain limited type of defined people. So it's a strong protection, but it's very narrow and it simply has no application to this case.

And I particularly commend your Honor to read, for example, the in re iPhone decision by Judge Coe. She did a very splendid job of walking through the case law and the ramifications of determining the sort of communications that would apply here. But plaintiffs still assert it and they twist themselves in knots a little bit.

So the Communications Act only applies to electronic storage, as I just articulated, and electronic storage means any temporary intermediate or intermediate storage. Well, we know that does not apply here because they're claiming that these cookies enabled something that occurred over time and enabled either interception over time, collection over time, correlation of information over time. It wasn't something that was done briefly. The cookies were placed on browsers and they stayed there. That's what they allege. So there's nothing intermediate.

And the other component of the definition is that it's stored by a communication, an electronic communication service for the purpose of backup protection. Well, cookies aren't placed for backup protection. It does not make any sense.

But beyond missing that -- on that sort of basic

elemental problem with these cookies not being on electronic storage, they can't allege that there are any SCA, Stored Communications Act covered facilities here. The SCA only applies to communications that an electronic communication server is storing in its own facilities, facilities that it provided. Nothing like that has been or could be alleged here, and as I mentioned, a long line of cases have rejected claims that things like mobile phones and personal devices, and, in facts, cookies, are covered facilities under the, under the Stored Communications Act, and every case that has thoughtfully analyzed this question has come out in that direction. There are a few outliers. I don't know how they reach that conclusion, but any case, if you look at them, these are not one-line decisions. Particularly the iPhone case I really do commend your Honor to read. It's a very lengthy review and analysis and I think it's very clear.

SCA covered facilities are things like the information that electronic communications service providers store on their own facilities, so what, what an Internet service provider, where it stores its e-mail. And it's designed to protect against having someone breakthrough security protocols, breakthrough and go into that server and get e-mail, things like that, in temporary storage.

Plaintiffs seem to recognize the problem with their allegations in their complaint because they make a

totally different argument in their opposition. In their opposition they don't argue that the facility are the cookies. They argue that -- I'm a little bit confused by their argument, but let's see. It's something like Google is the provider of the electronic communication. Plaintiffs' browser managed files are part of Google's facilities and the cookies are temporarily stored. That does not work for all the reasons I just described, but I want to highlight one of the real problems with this for plaintiffs' claim.

There's an exception under the Wiretap Act -- sorry, under the Stored Communications Act. 18 U.S.C. 2701 (c)(1). 18 U.S.C. 2701(c)(1). And it says that the bar on access to the stored communication doesn't apply to the electronic communication service provider that's providing the service.

So under plaintiffs', this new theory in the opposition where Google is the ECS provider, even if you could imagine the SCA, the Stored Communications Act claim applying, Google would have been authorized to get access to those cookies because plaintiffs' computers were Google's facilities under this, but it actually gets worse for their position because the statute also says that Google in that circumstance would be allowed to give third parties access to their computers because that authorization is not

just for the provider, but it's anyone the provider authorizes.

And there are other components of the statute that wouldn't make much sense. Plaintiffs would be subject to compel disclosure of these files to the government under 18 U.S.C. 273(a). Their argument just does not make sense and for good reason. The Stored Communications Act was never designed for this sort of case and it's why Courts consistently rejected it.

So those are the first two federal claims. I'm going to move on to the last federal claim, and that's the Computer Fraud and Abuse Act.

There are a lot of very technical components to this statute, but I think we can resolve it just by looking at the standing provision in the statute, and so I'm going to focus on that. The rest of it is brief in our papers. If your Honor has questions, I am happy to answer them.

Unlike Article III, where you have to allege a concrete injury that's particularized and traceable, which plaintiffs have not done, just doing that wouldn't get you a CFAA claim. Congress was clear that not everything that violated the technical words of the statute would be enough to get one into court. There's a $5,000 jurisdictional limit. You have to have been damaged or suffered loss in

the amount of $5,000 in order to state a CFAA claim.

And damage and loss are defined terms and they're limited to economic damages. It's an actual detriment to you. It's not a benefit to someone else. It's a detriment to you.

Damage is defined as any impairment to the integrity or availability of data, a program, a system or information. We don't have to spend any more time on damage because plaintiffs didn't allege any in their complaint. They do come back again in their opposition, maybe they recognize this problem and make a new argument. Can't be credited. It's not in their complaint, but I will just tell you, they claim that the planting of these cookies somehow impaired the operation of their browsers. That's not true. The browsers operated just as they were designed to operate, and their complaint makes that very clear. Their complaint includes the information either in the complaint or what they attached. The subject of our request for judicial notice, that's unopposed. Exactly how these browsers operated. Nothing was impaired. They weren't unable to visit websites. They continued to operate just as they were designed to. But, in any event, that wouldn't be a basis for denying the motion because it's not in a complaint at this point.

Loss. The other way you can get to $5,000 if

you actually have suffered any injury is defined as a reason, any reasonable cost to any victim, including the cost of responding to an offense, conducting a damages estimate and restoring data, program, system or information to its condition prior to the offense and any revenue lost, costs incurred or other consequential damages incurred because of interruption of service. So that last clause is quite important. Lost revenue, cost incurred or other consequential damages have to be due to an interruption of service.

Now, plaintiffs have not alleged any quantifiable damage at all, so there would be no way for the Court to even infer that anything could get them to $5,000, but I'd say there's no way they can allege at all ever loss under this statute. Economic damages this way, there's no way they had loss. If everything happened exactly as they allege, and this is a motion to dismiss, so we're going to operate in that world, all they had to do was clear their cookies. That does not cost anything, first of all. So there's no way they get to $5,000.

And, second, courts have routinely held that the unauthorized collection, use, and disclosure of genuinely personal information, like people's names, things like that, not the browser-generated information that's being sent here -- Courts have routinely held that's not a cognizable

loss under the CFAA, and I point to your Honor to the DelVecchio versus Amazon decision. This is actually DelVecchio 2. There are two of those cases, both important for different reasons.

IPhone, again, 2 and Double Click. I think the fact that there's iPhone 2 and DelVecchio 2 is a good identifier that these cases tend to get dismissed the first time around and they often get dismissed the second time around, too. You see multiple decisions coming out because plaintiffs, they're grasping at a way to try to a certain harm under statutes that don't typically fit. I would commend you to DelVecchio versus Amazon, the second of those opinions, and the DelVecchio case.

There are other ways which they have problems. We don't think we need to go into it right now. It's very extensively briefed, particularly in the Vibrant brief, that they can't aggregate properly here. But as I think I learned when I was quite young, zero times anything is still zero, so aggregation is somewhat irrelevant at this stage of the argument.

There are a number of claims that are asserted only against Google, so the claim that I just walked through, the Wiretap Act claim, the interception claim, which is vitiated by the fact that it's sent directly to the services, Stored Communications Act claim, vitiated because

no electronic storage, no facilities, and Computer Fraud and Abuse Act claim, vitiated because no damages at all let alone $5,000 damage or loss. Those apply to all the defendants.

The remaining causes of action that I'm going to go through, I'm going to try to be brief here, apply to Google, and there are two that are analogs to certain of the federal claims.

The first of the analogs, the Computer Fraud and Abuse Act. It's California computer crime law. That claim also requires damage or loss. It does not have the $5,000 jurisdictional threshold, but it still requires actual quantifiable damage or loss.

Here, there's no quantifiable damage or loss. All we have here is an allegation of a lost opportunity to sell personal value, to sell personal information at full value without an explanation of what the market is, without an explanation of who offered the information for sale, who offered to buy it, and the fact that it was diminished in value because of the events alleged here. That would be something like the buyer heard about this and said, oh, I was going to offer you X, but now I'm going to offer you X minus Y. Those facts are implausible and they have not been alleged, but the current allegations don't meet the threshold that is required. So the California computer

crime cause of action also doesn't seem to proceed.

And multiple courts have, when they dismissed a federal Computer Fraud and Abuse Act claim, have dismissed its tagalong state claim as well. I can point you to the Nextel case from 2012 in California.

And similarly there's a California invasion of privacy claim. That is essentially the California version of the Wiretap Act. The only difference is that it's an all party consent statute, but the communication that was intercepted here at the complaint on a, on a very straight read of the four corners of the complaint, it's very clear that this is the communication that was a sent to the parties, to the defendants, rather. There are only two parties to that communication, and when you send something directly to someone else, you're consenting to their receipt of it.

So the California invasion of privacy claim goes away. Plaintiffs have also alleged two California common law invasion of privacy claims, one denominated invasion of privacy. They both overlap. They didn't dispute that in their opposition. I don't think they'll dispute it today.

They have to allege that Google invaded a legally private matter in a highly, that would be highly offensive to a reasonable person constituting a serious invasion of privacy. Well, it's not a legally private

matter if you are sending it to a website in the first place, and I think the most on point case to which I would direct your Honor's attention to, there are two of them, is the Lowe versus LinkedIn case, which notes that California sets a high bar for invasion of privacy claims, and has noted that disclosure of browsing history is not highly offensive.

But I think perhaps given that the plaintiffs' claim has this disconnect in it, they -- they're upset about the way cookies are placed on their browser, but their complaint is mostly about the sending of information or the correlation of it to send to, send more targeted ads, which is done all the time. It's totally ubiquitous and it's well-known.

I want to read a case, read a small quote. I'm loathe to do this. I think this is actually quite instructive from the California Court of Appeals, Folcstrum versus Lamps Plus, a 2011 case. This is the California Court of Appeals.

We have found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiffs' private information which did not also allege the use of plaintiffs' information was highly offensive. However questionable, the means employed to obtain plaintiffs', here, address. There is no allegation that

Lamps Plus used the address once obtained for an offensive or improper purpose. And here, using information to send, anonymous information to send, rather, to display targeted ads isn't an improper or offensive purpose. It does not offend the senses under California law. It happens every day all the way. It's totally routine and there's nothing offensive about it.

Cases where drug prescription information was correlated has been found not to be offensive and that's far more personal than some browsing histories can be.

The other claims are a little bit perplexing. The California Legal Remedies Act, I was -- I was surprised to see in the complaint even a stretch as compared to many of the other ones. It applies only when there's a transaction involving tangible chattels and damage in the form of an increased cost or burden. It does not fit here, and it's for that reason that multiple courts have ruled that it does not apply to software services. It just does not apply to software.

Plaintiffs came back. They're listed in software, this is a service, and we were buying something with cookies. I honestly didn't understand the response, but, in any event, the California Legal Remedies Act categorically, is categorically inapplicable to software. Multiple California courts have said that.

So we don't need to get into the fact that there was no transaction here, and if you even assume there was a transaction, what was the cost to begin with, because there was no cost and how could it have increased? It's a little bit mind-bending when you think about how inapplicable it is.

Then we have the California Unfair Competition Law, which is another law you'll see when we read our brief, it's somewhat lengthily briefed. But like some of these other cases, you don't have to get past go the standing question. It, too, sets a standing bar that's higher than Article III. This was changed. It used to be quite different. There was a proposition that changed that, 7200, which is what this is.

You actually have to have had a loss of money or property in order to bring a claim under the unfair competition law, and Court upon Court have held, there's no loss of money, no loss of money alleged in this case. There's a vague statement that they lost the ability to sell, lost an opportunity to sell their information at full value. I don't know where to begin to look at that, because there's no -- it's not adorned with any facts.

They'll point to a bunch of studies and other things, but that does not say anything about these plaintiffs. The studies aren't about these plaintiffs.

They're not about real markets that these plaintiffs participated in and then started getting reduced offers about this.

This type of information doesn't diminish in value after one person collects it. This isn't the way the world works. It does not happen that way. So it's implausible. And so that's the money side.

And then data -- sorry, property. Multiple Courts have held, this was the prevailing law in California, there are no cases going the other way, that data, the loss of data isn't property under the unfair competition law, unless it's something like losing your Social Security number or something like that, but they don't allege that. They can't allege that because that information never would have been here.

So that brings us to the end, and we've walked through all the statutes and I appreciate you bearing with me on that. If you don't have any questions at the moment, I will sit down.

THE COURT: I do not have questions at the moment.

MR. RUBIN: Thank you.

THE COURT: Let's hear from plaintiffs.

MR. STRANGE: Your Honor, Brian Strange for the plaintiffs.

We have divided the argument among the plaintiffs with respect to standing first and then the Wiretap Act by Mr. Robertson, and Mr. Grygiel will address the other two federal claims, and then I will address the California claims.

As your Honor knows, we do have a settlement on a classwide basis with defendant PointRoll and we intend to file those motions for preliminary approval within 30 days.

THE COURT: All right. Thank you very much.

MR. STRANGE: Thank you, your Honor.

MR. ROBERTSON: Good afternoon, your Honor. May it please the Court, my name is Edward Robertson, and while Mr. Strange was here, we caught an audible and thought perhaps we ought to do the wiretap thing first. If the Court doesn't mind, we'll go that way.

THE COURT: All right.

MR. ROBERTSON: Your Honor, we've drawn this chart up, which is based on the pleadings, not things we found out since or otherwise. We believe this is all in the pleadings and there's a lot of this with which we agree with Google and its counsel.

There is at the beginning, Safari is obviously the Apple Internet browser. It has a built-in do not track device in it. It sends off, if I want to go look at the

Wall Street Journal, it sends off a get request to the Wall Street Journal. It says, send me your entire web page.

Now, the Wall Street Journal has a deal with Google, we're assuming here, that says we're going to let you have some of the space on our web page. It's called an iframe and it's blank, and you can put ads in there and money goes back and forth on that.

So the Wall Street Journal sends its web page back. Now, my law firm doesn't have a deal with Google. We don't send an iframe. So if you go to my little law firm, all you get is my little law firm's website back.

So Wall Street Journal also sends back to Safari, look, call up Google and tell them that you want to fill these holes in the web page. So Wall Street Journal is no longer in the communication. There is, as Mr. Rubin said, a call from Safari to Google, and I'm going to use call because I'm just a, not as technical as perhaps I should be, and says, fill up these iframes.

Google respond and says, okay, I will fill up the iframes. So then there's this communication that takes place between the two in which the iframes are filled.

Now, that's as far as Google's argument went today. That's benign. We don't think there's any problem there and that's not what the case is about. If that's all

it were about, we wouldn't be here. But it's about a little bit more than that because, as I said earlier, Safari has a built-in program in it that says, you can't put these drt cookies on a Safari web browser. Now, the drt cookies are these tracking cookies, as we call them in the complaint. So it has this built-in brick wall and that's how it's designed to operate.

So while Google is filling in these holes on the web page, it's also trying to send a drt cookie to Safari and Safari is designed to block it. But Google knows something. When you buy something and you have to fill out a form, you've got to be able to get that form back and forth. And so in order to defeat the brick wall -- and this is what we plead -- they send this invisible form that tricks Safari, that's the word we use, into thinking that it's not a drt cookie, that instead it's this form, and Safari has to let that happen or you can't do some transactions you want to do on the Internet.

So it gets by the brick wall through this device of the invisible form and it goes into Safari and now the tracking cookie is set and it can now track what happens on that computer.

So once it's in, it can track. Now, that's what we claim, your Honor, is the problem in this case, is this getting around the built-in thing in Safari and the Internet

Explorer, to keep that tracking cookie from going in, unless you affirmatively say you can do that if you want as a computer user.

So I'm going to talk to you, your Honor, about the Wiretap Act. And Pharmatrak sets out the elements. It's just a statutory case for you, your Honor. It's a statutory interpretation case. What are the elements? And Pharmatrak identifies five. Some other cases say there might only be four, but they are intentionally, an intentional act. We've pled that. We think when you send a trick, a piece of software in there, you know you're doing that, so it's not that they didn't know.

Secondly, there has to be an interception. We're going to talk a little bit more about that.

Third, there has to be an interception of contents.

And, fourth, there has to be an electronic communication and Pharmatrak says by a device. That's the fifth element.

So we've pled all of that. I don't think there's any question about that. Those words actually show up and the good news is Pharmatrak existed when we started pleading this and we knew what to write down.

So they come in and say, well, we've got two things. We've got consent here or we're a party. Now, the

consent they talk about in their first set of papers is, the Wall Street Journal gave us consent, but the Wall Street Journal is out of this conversation by the time that the Google Safari is taking place. All that's left is this conversation, Mr. Rubin is right about that. There's a call made from Safari to Google.

Now, iPhone has some interesting language in it. It says that there can be limited conversations. If you call the plumber and say, come to my house, I want you to fix the plumbing in my kitchen, I have a leak, that doesn't give the plumber the right to roam around your house, check your mail, look in the garage, go upstairs into your bedroom. The plumber is given limited consent. You may enter my house to fix the plumbing in the kitchen.

What happens when Google sets this tracking device, it's as though the plumber leaves a bug. And we say in paragraph 98 that there are other things that are collected and they are personal information. It's not just URLs. If it was, it would have no value. They have to know what you are doing in order to have these targeted ads. They have to know whether you're going to go to the Walmart ad, website, or Neiman Marcus, so the next time you get on, you get something from an expensive purveyor of goods rather than an inexpensive one. The reason this stuff has value is it tells them about me, it tells them about you, and that's

what this cookie does we say in the pleadings.

And that is why we think it violates the Wiretap Act. That is content. It's intercepted. It's intercepted when the plumber is in the house during the first phone call, when it's trying to break in because they find out stuff then. And then when a plumber leaves, the bug is there. And every time Google shows up, it finds out where you've been. There's a long list of the things that it tracks we plead in paragraph 98.

So two interceptions take place: The interception when the plumber is there and the interception when the plumber is not there and gone.

Now, I think that is basically it in a nutshell, your Honor. The conversation directly between Safari and Google is a limited conversation.

Now, if your Honor reads the statute to say that once you can talk about something, you can talk about everything, then you ought to sustain this motion to dismiss. But if the statute, and the consent language in Pharmatrak is very close to what we're talking about says, there is limited consent. You can't simply just get in for a penny and be in for a pound. If you are in for a penny, you're in for a penny. And here it was more than that. Not only was there a limitation on the conversation, but there was an express denial of the right to talk about more, and

that's what we pled happened here.

So the party exception has to be limited in some way or else it becomes meaningless. The consent exception has to be limited in some way or else it becomes meaningless. And the fact of the matter is, Google makes lots of money because this stuff that they say is just a string of numbers tells them all they need to know about me, and that what we say violates the Wiretap Act.

Now, I've got some more slides here that are more complicated, but I think given the time the Court has heard already, we'll move on to the other causes of action. But there's harm here because the statute has some provisions for injunctive relief and some fines.

I thank the Court for its time.

THE COURT: All right. Thank you very much.

MR. GRYGIEL: Good afternoon your Honor.

THE COURT: Good afternoon.

MR. GRYGIEL: Steve Grygiel.

I lost count at one point during my friend, Mike Rubin's argument, about how many times I heard how the Internet worked. All I could think of was when I was hearing that was, sounds like a factual question to me, because as your Honor has written in three recent opinions dealing with the pleading standards, factual allegations in the complaint are taken as true, and your Honor in three

recent cases, including Wilmington Trust and including Senju Pharmaceuticals and the RICO case has said that under Ericsson versus Partis, the plaintiffs' factual allegations are taken as true.

So we have to start this entire discussion from that proposition. And in this case, what we are talking about is that the defendant here, Google and the other defendants, are saying that a multi-step process done in secret of technological ledger domain that defies easy description is something they had every right to do. It's something that wasn't blocked by what we allege was the blocking device in place. That by itself, your Honor, shows that this motion to dismiss, all of the motions to dismiss should fail, because the complaint alleges that blocking was in place, and it alleges factually that the defendants intentionally got around it.

As the Pharmatrak case says, your Honor, when there is a financial motive for someone to get unauthorized access, you can pretty much take it to the bank that that access was unauthorized.

Anyway, let's talk about standing a little bit. Mr. Rubin was talking about standing and I think he made a couple of mistakes and I think a couple of them are of constitutional dimension.

The first one begins with, conflating merits in

standing. In the cases that the plaintiffs cite and in the cases that the defendants cite, we know one thing for a truth. Warth versus Seldin tells us this. The merits and standing are separate increase. Standing is first.

We know what Judge Alito told us before he was Justice Alito. Standing is not Mount Everest. We know in the United States versus Scrap decision and in the Third Circuit's Echo decision, In re Google Industries, we know that an identifiable trifle of harm suffices for standing.

You do not under any constitutional regime that this Supreme Court in the last two years has been thinking about take the merits and say they can't get there, so therefore they don't have standing. No standing is first.

What do we allege? We've alleged two things. We have alleged two categories of things. One, statutory violations. Number two, we have alleged the deprivation of the full value of our personally identifiable information.

Let me take the statutory standing first. And I think there is, as happened in many of the cases Mr. Rubin has cited, there is the effort by defendants to conflate statutory standing with Article III standing in a way that makes it a two-tiered standing requirement. Essentially says, you have the invasion of the statutory right, which Warth versus Seldin tells us, is enough to make out a claim

for standing. But the defendant says, but PII is not worth anything, Judge. At least we don't think they've pled it, so they don't have standing.

Not so. Under the Wiretap Act and the Stored Communications Act and under Warth versus Seldin, all that is needed to state a statutory claim for purposes of standing, to open this courthouse door, is the invasion of a statutory right that is your right. We have alleged that these plaintiffs have the right to be protected by the Wiretap Act and the Stored Communications Act and the Computer Fraud and Abuse Act and that an intrusion upon that right, even if nothing more, even if nothing more happened, is enough. And we have a great example of that, your Honor, right here in the Third Circuit, and that's the Austin Countrywide case. Essentially, as your Honor might remember, that is a case that deals with real estate transactions and the RESPA statute.

And what the Third Circuit essentially said there, and I'm quite sure a reading of that case will bear me out, is that the statute gives a person who is a participant in a real estate transaction the right to a transaction that is free of conflict of interest. Well, the defendants in that case said, the bank, well, Judge, why do the plaintiffs care? It didn't cost them any more money. And the Court properly reading Warth and all of the cases

that have followed Warth said, they're entitled to an interest, conflict of interest-free transaction. They didn't get it. Ergo, they have standing.

In these cases, your Honor, Congress in its infinite wisdom has decided that the plaintiffs have standing and that is enough. There is nothing more that is required, try as the defendants might to add something to the requirement for standing. It's just not so.

If I can move on, your Honor, to the question of the personally identifiable information, with respect to the standing for the Computer Fraud and Abuse Act, which I will come to substantively in a moment. Personally identifiable information is something we do allege that these plaintiffs had and were deprived of. When your Honor looks at paragraphs 1 and 2 of the complaint and couples that with, I believe it's paragraphs 10 to 13, the only possible inference according to the term of the language that we use is that these plaintiffs were using the Internet in a way that resulted in the deposit of these cookies that were supposed to be blocked.

Then the question is, okay. They've got these cookies. How are they damaged? We'd say a couple of ways, your Honor. In all of the other cases, the litany of cases, many of which took place long before the market in Internet data has boomed the way it has now, and many of these cases,

for many example, iPhone I think is 2001, you didn't have something you have in this case. It's a fact that's crucial, and that is the fact of the block. The block helps to define the value proposition.

If I leave my painting out on the front walk and I don't do anything to protect it, it's a fair inference that I don't assign a great value to that painting. But if I have it behind a block, behind a locked door, the value proposition then is much more reasonable and certainly an inference to which plaintiffs are entitled in a case like this, that they had put their personally identifiable information, described at paragraph 98, in great detail and footnote 67 to 98, that that information has value.

Now, the defendants say, as they do, well, Judge, they cite a bunch of studies, but all the case go the other way and, your Honor, I'm not going to belabor them in detail because your Honor I'm sure has read them. But when one looks carefully at a case like Claridge versus Rockview, that case did not say the personally identifiable information can never have any value in a monetary or monetizable way. What that case said in fairness was, there's a paucity of information and at this stage of the pleadings, I'm not going to toss the case on that basis. Double Click refused to dismiss the case on the basis of PII not having value. The LaCourt case noted for example, I

believe it was the tepid allegations, the half-hearted -- I'm quoting -- efforts made by the plaintiffs to show value. We have a complaint that is full, yes, of studies that show what the value is in the marketplace for this data, including value that Google has assigned to it.

We allege much more than those complaints. That takes us out of the realm of a generalized, completely conclusory allegation that has value. We're showing in the marketplace for this information, people pay for it. And when you look at the inferences here to which the plaintiffs are entitled, for example, that Google, Vibrant and MIG and WPT businesses depend wholly on the collection, slicing, dicing and selling of that data, it's pretty easy to see that it has value.

Now, Mr. Rubin will say, and the argument gets made, well, Judge, it may have value to me, but it's not lost to them. Well, the answer to that is twofold. Certainly, under the statutes, it is. The Computer Fraud and Abuse Act just says information. It doesn't say proprietary information. It doesn't say valuable information; just says information. There are certain things you don't get to have whether that information you think is valuable or not, certain information you just don't get to take for nothing.

And the second issue is, how could we sell it?

It has already been sold. I don't have to make an allegation when someone steals my car that I had tried to sell it before and therefore I can tell the police officer that my car was worth $7,000. That just doesn't add up. That's not, to quote Mr. Rubin, the way it works. We're entitled to allege that. We have alleged it as a fact. Discovery will show that these items of information have value.

And, again, here, your Honor, we're here on a motion to dismiss, not summary judgment. And on a motion to dismiss, as the Phillips Third Circuit Court told us, all the plaintiffs have to do is raise a right to relief above a speculative level such that there's a reasonable inference that discovery will produce evidence of the required elements. And in this case, rife with the detail of facts in this complaint, I submit, your Honor, it's very difficult to come to any conclusion but that we have pled a plausible case and that we have certainly pled standing.

To me, it's, in fact, inconceivable that we have not pled standing in a case where the irreducible constitutional minimum of injury in fact is satisfied simply by the statutory violation and the cases that recognize, on less detailed complaints than ours, that PII can have value.

Finally, on standing, your Honor, we heard a

lot -- not a lot. We heard some about the requests for judicial admissions that we're not opposing. No, they were not opposed. I loved them. I would take every word in those statements and those requests for judicial admission: Mr. Myers' web blog of February 17th, the Wall Street Journal article of the 17th, Google's privacy policy, and ask your Honor upon reading that whether or not what the plaintiff alleged here makes perfect sense. What those say in a nutshell is, cookies track. They don't say cookies are these innocuous benign beings, the mere nuts and bolts of cyberspace. They all speak of trackable cookies, cookies that permit, as paragraph 98 says, tracking of information.

A second thing they say is, Google and the other defendants did this on purpose. They did it intentionally. That takes care of the intent element in every single claim we have here.

The third thing they say is, they did it for money.

And the fourth thing they say is that, and all of the quotes in the complaint make it clear, none of the defendants, when they got caught doing it, said, hey, you knew about it. We have a right to this. You should not be bothered, you knew about it. What did Vibrant say? The hack was a work around. A workaround? It sounds like a hack to me, designed to make Safari work like every other

browser, meaning no default setting. Well, that's an admission.

What we have from Rachel Whetstone, who was Google's spokesperson, was very simple. She said, we created a temporary communications bridge essentially between two Google domains. Well, you'll see in the request for judicial notice materials, Mr. Myers' blog, he explains exactly how that leads to the surreptitious grabbing up of information that the Safari browser was designed to block.

And I would say, your Honor, at the end of all of that, those are all fact questions, if they are not fully clear enough from the pleadings. Those are all enough to suggest a right to relief. It's far above a speculative level.

So on standing, your Honor, I think statutory standing, they simply have it wrong on the law, and, in fact, I like that they cite Lowe versus LinkedIn, because Judge Coe there in her second opinion cites Massachusetts versus EPA, which I won't read, but is, your Honor, I think the best phrasing I've heard of exactly what statutory standing means and basically it is somebody violated a right. You're protected by the right and you don't need anything more to get inside of that courthouse door.

Now, your Honor, I'm going to turn, if I may, to the question just at the top here of the Stored

Communications Act. Chief argument, one of the chief arguments Mr. Rubin made, and it's not without its appeal, so I can understand the Court paying close attention to it, is that, well, Judge, the Stored Communications Acts deals solely with information in Stored and the Wiretap Act deals with information in flight that is being seized contemporaneously with its transmission. How can you plead one and not the other?

Well, your Honor, there is an answer to that, and the answer to that is as follows. Actually, it has got a couple of parts.

The first answer is, the United States versus Councilman, Councilman Roman Numeral III, the en banc decision Justice Lopez wrote, says, while it may seem a semantic paradox, it is not a technical paradox. Information in a packet-switching regime, which is what this is, can be both simultaneously in transient temporary intermediate storage as well as in flight en route to its final destination.

So the dichotomy between information for purposes of the Stored Communications Act being in temporary intermediate storage incidental to transmission, and on the other side, information in flight for the Wiretap Act is a false dichotomy. And a couple of cases have recognized that. For example, one of the cases that the defendants

cite here, United States versus Smith, makes that point. The case is not on all fours and I don't pretend to your Honor that it is, but it makes a very interesting point.

It says that the Wiretap Act and the Stored Communications Act, for purposes of protecting communications, different, but not temporally, because it's the temporal difference that Mr. Rubin and the defendants point to is making them mutually exclusive. No. What that case says is the wiretap's act intercept concept protects information that is in flight and that someone is grabbing up, if I can use that kind of clumsy gesture, which I realize it is. The Stored Communications Act deals with getting in a position to grab up information and Smith can be read, I think, quite fairly to say that they are not mutually exclusive.

And I think, as we step back and say, well, what exactly are these areas of the law protecting and what is the purpose of these statutes, interpreting those statutes consistent with their aim, one of our, of course, chief operations leads to the conclusion that there is not inconsistency between pleading the two. If you plead one, you are not out of court on the other.

And finally, your Honor, apart from those cases, the Intuit case says the same thing, by the way. Intuit says for our motion to dismiss, I'm not going to dismiss on

that basis. Intuit says you can have some communications that are in flight that got intercepted and some that are in storage that are subject to the Stored Communications Act.

On a motion to dismiss, they've pled enough. Our case is certainly as strong as that for purposes of pleading a claim there and for getting around this false dichotomy of mutual exclusion.

And, finally, there's a statutory definition issue. And this doesn't get discussed much and I apologize if I didn't make much of it in our brief. I'm sorry. I can't remember if I did. But under the statute, the definitions I believe are 2511. But the statute's definition apply both to Wiretap Act and Stored Communications act. And there is an exception to Wiretap Act communication for information that is stored regarding electronic funds transferred. That exception would be completely unnecessary if the Wiretap Act did not cover certain stored communication. It's not a point that gets played a lot, but it intrigues me. If nothing else, it shows that the support that Smith gives us and the support that Intuit gives us and the support that Councilman gives us is proper support.

Anyway, I will turn now, your Honor, to the, unless your Honor has any questions, to the Stored Communications Act.

THE COURT: You may continue.

MR. GRYGIEL: The Stored Communications Act. If you could get that slide up, Jim. My fault. The one with the elements in it.

Here we are. The Wiretap Act's elements are one thing. The Stored Communications Act are another. Intentionally accesses is the first one, your Honor. I don't think that can be seriously contested here. Look at the request for materials in judicial admission, you make it abundantly clear this was intentional.

A bank doesn't rob itself. A cake doesn't bake itself. This was a multi-step process that Mr. Meyer and Mr. Naryian (phonetic) and Mr. Shokai (phonetic) of the Wall Street Journal confirmed was intentional. And as to Google, they're clearly intentional. Vibrant and MIG, they say all inferences support that.

Without authorization. Nobody has pled consent in this case and they can't because the users didn't give consent and out complaint says otherwise. Our complaint says not only didn't we give consent, we did not know about it.

Google says it was a known loophole in Safari. Well, known to whom? First is a fact question. Second, according to this request for judicial notice, in order to be valid, Software Wizard. Not like me clicking on the

Internet at night looking to buy my kid a hockey step. Completely different. There's no authorization there.

A facility. And we get into the question about what's a facility, and here we get to some technical stuff. I will just make the following points. First of all, facility is an undefined term. Facility is a little bit amorphous. I can think of a car or a bus, and then I can think of a car service if I'm in New York or a bus service if I'm in up state New York, like where I grew up. But a facility is an undefined term, and there are a number of cases, including cases that Google likes, that say that what we have here is a facility. Our browser managed files. That's what our complaint says.

The Chance case says that the Stored Communications Act's definition of facilities includes personal computers. The Intuit privacy litigation says, Section 2701 does not require that plaintiffs' computers be communication service providers, only that they be a facility through which an electronic communication service is provided. Export Janitorial cites Intuit and says, plaintiffs' computers on which the data was stored may constitute facilities under the CFAA. Council on American Public Relations. Congress intended facility to include the physical equipment used to facilitate electronic communications. Browser managed file equipment, helping to

move communications around the Internet. That's facility. And the cases say so. They don't all say so. The cases go both ways. But on a motion to dismiss with the facts as we have alleged them, we have alleged the facility under the Stored Communications Act.

When we get to the question of through which an electronic communication service is provided, we get to yet another definitional hurdle. What's an electronic communication service? Well, here, the statute actually gives us a little help. The statute gives us definition. I won't quote it exactly unless I would have it on the slide, which means I should click this. I shouldn't. I might have removed it.

An electronic communication service is something that enables a user to send or receive electronic communications. We allege in the complaint in facts that control that the electronic communications server, service, is the browsers. Why do we say that? Because the Safari browser and the Internet Explorer enable, permit users to send and receive electronic communications.

And on pages -- I'm picking on Google here, I think it's about 22 through 26 of their brief, they're quite clear to talk about how browsers permit the interface of a user with the Internet, in particular, in the exchange of electronic communications. I would submit to your Honor

that that is a perfect admission of something that's perfectly sensible. These terms need to be interpreted in light A of their statutory purposes, which is to protect privacy. I don't think anybody decides that.

And, second, there's no technical strain at all to say that these browsers are the electronic communications services.

We do argue in our brief, we say, not exclusively, but Google is also an electronic communications service. That's also true. Google helps people communicate and get and receive electronic communications, but we don't say that exclusively. And the tension comes in, which is not for the plaintiffs' prejudice, because Google became a party to a part of the conversation that it wasn't supposed to be a party to. That is why you have both the browsers being the services as well as our brief statement, in our brief statement, saying that Google is.

An electronic communication. There's a definition for that in the statute and I don't think, your Honor, anybody disputes that the transmission of the information we've alleged in this complaint is electronic communications. Get requests, these secondary get requests. A post. The transmission of a secret form. These are electronic communications well within the act, and beyond that, the information that paragraph 98 says, the cookies

allowed to be associated with particular users are also electronic communications.

And on that point, your Honor, United States versus Forrester, it's Footnote 6. I regret that it's a footnote, but Footnote 6, it's a very useful discussion of why it is that an URL, which Mr. Rubin disdained, but why it is that a URL is actually content, why that is meaningful information.

And what it essentially says is, it tells people something about you. If you type in www.Help For Drunks or Help for Incest Survivors survivors, somebody who knows that about you, then they can populate an ad space with relevant information, they know a lot about you. That's different from just the kind of cases the defendant cite that talk about the time of a call and how long it lasted. It's very different.

And then we come down to storage. What does it mean to be in storage? And here again we have a difference of opinion with the defendants about what it means to be in storage. It's not as broadly defined as electronic communication.

Electronic storage, for purposes of the statute, means in temporary storage, intermediate storage, and they are not disjunctive. They're all together. Temporary, intermediate storage that is incidental to the transmission

of the message.

And I would simply say the following on that, your Honor. At paragraph 218 of our complaint, we allege how the information that we say is subject to our claims was being taken contemporaneously. Among other things, this was recently updated information. It wasn't in permanent storage.

Number two, the defendants themselves say, and this is in their briefing, that this cookie that caused all the trouble was an intermediate cookie. Intermediate cookie, intermediate storage.

Ms. Whetstone, when they got caught doing what they got caught doing and stopped immediately, said this was a temporary -- sounds like temporary to me -- communications bridge. Out of Google's own mouth, we have the temporariness of the storage that we need here.

Apart from that, your Honor, we also have cases that talk about what electronic storage is, and those details in our complaint, which are factual and entitled to the presumption of truth, are borne out not only by every inference that attaches to those facts, but also to some cases.

Expert Janitorial, and I will read it because I think, to borrow from Mr. Rubin, it's an instructive quote. For purposes of a motion to dismiss plaintiffs' allegations

under the SCA that the e-mail accounts, user names and passwords were stored on plaintiffs' computers and that defendants knowingly accessed this stored information without authorization are sufficient allegations to assert a claim under Section 2701, an appellate claim.

Intuit. Plaintiffs have alleged that defendant accessed data contained in cookies, just like here. That it placed in plaintiffs' computers electronic storage. The Court concludes that this allegation satisfies the liberal requirements of Rule 8A2.

So we know that we have here electronic communications in storage that were taken without authorization and without consent. That's the Stored Communications Act. And to the extent the numerous contesting facts in the brief say anything, what they say is here, that discovery is merited. This isn't summary judgment. It's a question of, have we stated sufficient facts to make them plausible. And when Internet gurus like Mr. Meyer and Mr. Miller, Doug Miller, whom we quote, as well as the defendants' own spokes people say, well, we did it and here's what we were doing, that's more than plausible. That's a question of, let's get the discovery and see how much more there is here.

I'd like to turn, your Honor, now, to the Computer Fraud and Abuse Act.

A couple things I'd like to say before I talk about the elements. The defendants make a lot about it in their brief, I won't here, other than to state it.

Every one of the defendants is at pains to tell the Court, your Honor, it's an anti-hacking statute. It has very little to do with what went on here. The facts in the complaint say otherwise. The facts say it has everything to do with what went on here. This is no different than the prototypical hack. It's outside in with someone with great expertise victimizing someone who doesn't know who has erected technological barriers to prevent it from happening. In fact, when you look at the Craig's List case and the Facebook versus Power Venture case, they make that point. The circumvention of technological barriers is quite indicative of an offense, and that's exactly what happened here.

So the defendants like to say that that case has nothing to do with this case. We think the facts are completely the opposite. That's just characterization. That's spin. That's argument. That's not a fact entitled to a presumption of truth, particularly since it's the defendants who are saying it.

The second issue here, your Honor, the defendants say, Judge, if there's a problem, if there's any problem under the CFAA, and we think there isn't, we're

entitled to be excused under the rule of lenity, and the defendants cite various cases for that. Reocall is one.

Well, the rule of lenity applies when you have an amorphous statute that may have criminal consequences being applied either in a criminal or civil context. And the idea of rule of lenity, of course, as your Honor knows, is simply to say, we're not going to stick somebody with liability of conduct that they couldn't have reasonably foreseen.

The facts in the complaint show how big Google is, how sophisticated it is, its previous experiences with the FTC, which fined them $22.5 million for violating an order that was covered by the conduct here. They knew what they were doing.

Number three, again, this is the facts we pleaded and we're entitled to their inferences. They did it in secret. They did it a lot. They did it for money and they did it with technological wizardry, and together found a technological blog that they knew about and apparently the people in their world knew of it and nobody else knew did, using a forced submission rule that then triggered a one in/all in cookie blog.

It sounds pretty technical to me and I think that gets us over the hurdle not only of intent, but it also goes to show that the CFAA was violated. And it shows that

the rule of lenity has no business in this case. And defendants say Google, at page 26, I believe, said plaintiffs have not alleged any facts at all that show that Google altered a setting. That's pretty close to a quote.

I'm sorry to be flippant. I don't mean to be flippant, your Honor, but are you kidding me? That's exactly what we allege. You dismantled a default setting. We had the default on. You came in in the dark of night and turned it off. If you were entitled to it, you would have disclosed it, you would have gotten consent. You certainly wouldn't have done what you did and stopped doing it immediately and said, oh, this is temporary.

Anyway, back to the CFAA. The elements. Knowing transmission of a program, information, code or command. Mr. Rubin says they can't possibly allege it. Well, we alleged that a secret code embedded in the ads that Mr. Robertson described that were sent from the ad-serving company to the browser of the user, that those codes trigger a secret iframe. That secret iframe then sends an undisclosed form that essentially tricks the browser into thinking that the person at the keyboard is actually affirmatively communicating with this third party, which then lets the cookies come in, what Google calls the intermediary cookie then followed by the rest of them.

But the transmission of that code, described in detail, including with all the slashes and that indecipherable language that the web people use, it shows exactly how they did it. They transmitted a code to disable the blog.

Intentionally caused damage. Their intent is clear. Damage. Any impairment to the integrity of a system or a program. We had a system. We had a program that was the default system and they damaged it. They impaired it. And, by the way, the Black & Decker case, which is cited in Expert Janitorial, says that damage for purposes of CFAA doesn't require the loss, destruction or corruption of information. Damage for the CFAA, it's enough if you allege that a computer was made less secure. That's precisely the gravamen of what resulted from the defendants' conduct here. So we're there, certainly there for purposes of a motion to dismiss. Entitlement to discovery comes after.

Without authorization, we've talked about that with respect to the other elements. The secrecy itself takes care of that.

To a protected computer. Nobody disputes protected computer because that is simply something that's connected to the Internet and everybody knows what it is.

Exceeded authorized access and authorized and unauthorized access. Essentially, the same things. I won't

repeat myself here. They obtain information. It has got to be information, not special information; information. That's all it says. We have pled that. We're entitled to the truth of those factual allegations.

Now, if I can, your Honor, let me come just quickly to the remaining elements here that the defendants raised. The first thing they say is, well, Grygiel can't allege that a private party can aggregate the damages to the $5,000 threshold. That's reserved under the statute only through federal government prosecutions or investigations.

Well, first of all, I believe that misreads the statutory definition. The statutory definition describes loss, which is the operative provision for purposes of a civil action. Describes loss as any loss to any person, including, and then there is a chain of somewhat disparate elements, including physical injury, wrongful disruption of government files, and other items.

Well, my view is, statutory interpretation rules do apply, and what they say is the word including, after the following elements, after including, mean they're not exclusive. Those are simply suggestive. That is Massachusetts versus EPA. And our friend Justice Scalia has repeatedly made that point in any number of Supreme Court cases. So statutory interpretation shows us that we are

entitled to aggregate those losses.

Number two, Czech, the case Czech. That case says that the parenthetical that the defendants say in their briefs restricts the ability to aggregate to a government plaintiff is just wrong. It says that's a mistake, and it goes into the legislative history, which to quote Judge Leventhal opinion, it's like going into a party, kicking out your friends.

It says that legislative history snippet that defendants rely on and I believe Vibrant relies on at great length is of no moment, that simply permit this, not excludes it. The point is, your Honor, is statutory interpretation, your Honor, the plain language, any person, any loss, aggregate by itself suggests you can aggregate over a one-year period certainly suggests aggregation is reasonable. We have cases that we cited in our brief, I won't belabor, that make the same point. We're entitled to aggregate the damages to reach the $5,000.

The next thing the defendants say is, well, you've got to have a single act, and they say you can't possibly have a single act here to get to the $5,000, because look at all of these computers they talk about and look at all of these people and it can't possibly have been a single act. Well, we say, first of all, the single act appears nowhere as a restriction in the statute. That's

number one.

Number two, the single act is inconsistent with any loss to any person with the implication being multiple acts and multiple people over a one-year period. That certainly suggests that the single act requirement doesn't apply.

Third, creative computing. Freedom Bank Shares both say that is not an element of the statute. It does not apply.

The single act requirement, when you think about what that would mean, and one of the cases we've cited says this, it would essentially defeat the statutory purpose, because what it says is, a single computer hack causing $5,000 in losses would be actionable while systematic hacks repeated 30 times, each causing $4,999 would not be. And that makes no sense given the statutory purpose let alone the statutory language.

If Congress wanted to have a single act in the statute, they knew how to do it, and Congress didn't. Defendants, and Mr. Rubin pointed, out cites the language of economic losses only. That's all you get. The question is, what are economic losses? There are cases that we cite and cases that the defendants cite that take two different views of how broadly you can read losses for purposes of this CFAA. Those cases largely stem, your Honor, from an

intellectual dispute between the Ninth Circuit and the Seventh Circuit that has no relevance to why we're here today. That is the No Sale chain of cases which say, wait a minute. The CFAA is all about unauthorized access. It's not about misuse, and that is a narrower view. Those cases take a narrow view of damages.

The broader cases stemming from the Seventh Circuit's Citrin case say otherwise. They say that if I have access to a computer, but I start to misuse it when I'm in there, then the statute is triggered. Those cases tend to take a broader view. I say we can avoid that swamp, your Honor, which our cases tend to raise. We cited the Baxter case as a summary of them. We can avoid that by simply looking at the statutory language here, and what the statutory language says is clear. Any loss, any person, statutory language makes it clear.

Defendants say, they don't allege an interruption in service. Statutory interpretation principles in cases we cite say that the interruption in service limitation doesn't apply. That is a matter of statutory interpretation. That does not cover all the antecedent elements of this statute, which is aimed at protecting computer hacking, a statute that since its enactment has been consistently broadened in its scope, its definitions and its reach.

Finally, we cite cases. Urban and Smith is a good one. It is in our brief. E.F. Cultural Travel, Costar Realty and in re Toys-R-Us, all of which your Honor say, take a broad view of these losses. And if you argue that it has got to be a loss that affects the functionality of the machine, that's precisely what we allege. We say you dismantled our default setting and that by itself is what gets you there.

Finally, and I know Mr. Rubin will say this because he said it very eloquently, he's a very good lawyer. He's going to say, well, Judge, that may all be true, he's got some law, he's got some argument, but where does the money value?

And the answer to that is twofold, your Honor. First of all, we know it has value because the defendants, as we plead, it's a business proposition, collect it and sell it. We quote their businesspeople saying this is what they do. So we know it has value. As the value to us, all we need to say for purposes of a motion to dismiss is that we were deprived of the opportunity, which we don't have to actually go to exercise for purposes of the motion to dismiss, to capitalize the net value ourselves or to decide to keep it. It has value to me simply by virtue of the fact that it's private.

That, not to get too far afield, but one of the

things back to what Justice Brandeis said in Olmstead, the right to privacy is the single most valuable right to people, and there has been a lot of Supreme Court history following that with Katz and Rowe that make that very clear.

Discovery will show what its value is. I am sure when we do discovery in the case, we will see precisely how the damage models, how the algorithms developing the damage models for the defendants work. There will be no dispute, this information is extremely valuable and its deprivation to the plaintiffs is a loss cognizable under the Computer Fraud and Abuse Act.

I've been talking a long time, your Honor. If you have any questions, I'm happy to answer them. Otherwise, I will sit.

THE COURT: No. Thank you very much.

MR. GRYGIEL: You're welcome, your Honor.

MR. STRANGE: Your Honor, I will be brief. The frequent of these cases leads to the end of the argument the California claims, and they actually, when you read the opinions, put them at the end, some of them are a little bit confusing.

And when I started preparing with respect to the California computer crime law, which the real name is the Comprehensive Computer Data and Fraud Act, and the reason I

say that is, it's a very broad claim. When I started preparing, I realized that in the pleadings, a case not cited was my own case, which was decided a few months ago by Judge Rogers in the Northern District of California. And if you will forgive me, it's called Hernandez versus Path. And it's 2012, Westlaw, 519, 4120.

And Judge Rogers denied a motion to dismiss under this section, and in that case, the issue was whether, if you downloaded an app and the app took your address file without your knowledge, does that state a claim under the California Computer Crime Act?

This case is a classic case for that act, and the reason is, if you go back to the brick wall, where the consumers try to block the cookies, but as we explain in paragraph 93, Google sent an invisible form and a code accompanying it to trick the user's browsers into requesting this cookie, thereby getting access to the computer.

So if you just look at the plain language of that statute, for example, one provision of Section 502(c)(7) says, knowingly and without permission accesses any computer. If that's not knowingly and without permission to accessing our computer, I'm not sure what is. But just to quote from Judge Rogers' decision, she said, based on the current limited briefing, the Court cannot conclude as a matter of law whether past alleged conduct,

i.e., downloading the Path app, which plaintiff voluntarily installed on its mobile device, contained undisclosed software code that surreptitiously transferred data onto plaintiffs' mobile device to Path servers fall outside the scope of the California Computer Crime Law. So I think that under these facts, that we have alleged a claim under that section.

And as one of the cases that defendants quote, which is the LaCourt case, it notes that the California Computer Crime Law does not have a minimum damage requirement.

And there are two other minor points, your Honor. With respect to the California constitutional privacy claim, we've quoted in our briefs the language that the purpose of that constitutional amendment was the stockpiling of information that's personal to people. That the only California case that the defendants really rely on, their primary one, I should say, is the Focustrum case that I believe was quoted to you in the argument by Google's lawyer. But that case only involved someone's address, their physical address. That was given to Lamps Plus, who then sent them advertisements.

That case noted that some examples of violation of privacy would be disclosure of HIV status, would be confidential mental health records, would be the CHP, who

disseminated photographs on the Internet.

So if you think of the information on your browser, if you look at someone's browser history, what doctors they looked at. We gave the example of Help For Drunks. We have people checking HIV issues for themselves. That kind of private information, which the cookies allow you to correlate to your user, that is private information that I think clearly does fall within the ambit of that statute.

And then, finally, with respect to -- I'm just going to mention the UCL claim. I'm not going to address all of the arguments because I don't want you to think I agree with them, but I don't think we really have time here.

But just under the UCL claim, the unfair competition, which we deal with, of course, all the time, and Judge Rogers dealt with in her opinion, we have the unlawful prong, which Section 502 would be a predicate act of. And then we have the unfair and fraudulent prong.

So I think that we've satisfied the California claims for all the reasons we've set forth in our brief.

Thank you, your Honor. Appreciate your time.

THE COURT: Thank you very much. Mr. Rubin?

MR. RUBIN: I was going to start by saying I'm going to try to be brief, but people keep saying that.

There were some loose words used in a lot of that argument, and I want to make sure that we are all clear.

We are not arguing, and wouldn't argue at this stage of the case, that the Court should be considering anything outside of the complaint or the materials of the complaint referenced and relies upon. I think what I said was, their allegations about the get requests were right and how the Internet worked and then we saw a picture of how that worked.

I want to first address a few actual issues because I think they were relevant to all the claims and they're just not quite right.

First of all, we saw a picture of a brick wall. You know, there's always a bit of an issue when you try to import physical examples into the online world, but the brick wall isn't the right example here. The allegations that are in the complaint, so back to the four corners that the plaintiffs want us to focus on and that the rules say we are to be looking at.

The plaintiffs here alleged that they used these browsers in their default settings. They also allege that the default settings have exceptions. And if you look at the piece by Mr. Mayer, I believe it is Exhibit 3 to the RJN, there's a screen shot, picture, it's actually quite

well done, of the setting themselves. And it is very clear that one of the settings is never. That is, never accept cookies. That's not the setting that these individuals had. They had a setting that said something else.

THE COURT: But did they know that? I mean, I don't have any idea. I have no idea.

MR. RUBIN: I have no idea either, but it's part of the complaint. So the fact is, and right now we're assessing whether software interactions in their default state, when the default state has certain exceptions in it.

THE COURT: But, to me, that seems like an issue of fact. It's though, certainly, you're asking me to make legal conclusions, but the question is whether I can make legal conclusions without having a true understanding.

If there are undefined words, you need to have an understanding of how the Internet works in order to give the best definition, to order to give a legal conclusion. I'm not confident that this is the kind of case that it's easy to say that accepting all of the plaintiffs' factual allegations, I can still say there are no -- that your position doesn't have factual issues associated with it.

MR. RUBIN: Let me see if I can phrase it this way. There's no doubt that I would take issue with some of the, some of their characterizations, particularly some of the arguments and the way it was phrased up here, which is a

bit more hyperbolic than some of the statements made in the papers.

THE COURT: Always.

MR. RUBIN: Of course.

THE COURT: That's why we have oral argument, I guess.

MR. RUBIN: To make your argument less interesting. But what you can decide, and I think very clearly decide from the four corners of the complaint, and you don't have to get into any of this, because there's agreement on how -- this is in paragraph 41 of their complaint. The chart that they had up didn't have any paragraphs associated with it. But the only communication that's occurring between their browser and the services are the get requests.

There was a suggestion by them based on that chart, that after a cookie is placed, some additional communications occur. That's nowhere in the complaint. That's absolutely outside the complaint. The allegations alone will get you there.

But there are two other key points, and I will go back to the point I made at the outset of this hearing. Two points that require dismissal here, and it's the fact that they had not alleged any cognizable harm.

And if you look at the studies that they have,

that Mr. Grygiel pointed to, none of them are connected to these plaintiffs. These plaintiffs say, in the back of the complaint, paragraph 220-something, I believe, that they lost the opportunity to sell their information for full value. That alone is too threadbare of an allegation to provide this Court with jurisdiction over the matter.

And I want to make sure that our position with respect to why they can't proceed based on the recitation of the statutory claim is clear, because I think it has been muddied a little bit. I'm sure it wasn't deliberate, but I want to make sure.

We aren't saying -- and this is an issue that is bubbling around in courts -- that even if you check all the boxes for a statute, you meet every single element, but you lack Article III injury, you have no personal injury, the fact that the statute itself provides for some damage amount, our argument is in that case, no, you wouldn't have standing.

That's not the argument we're making here. We don't need to make that argument here because they can't check the boxes on those elements. And that is not looking into the merits of the case, and none of the cases they cite say that that is looking into the merits of the case.

It would be a different thing if they were able to show that all of those situations had been met or that

none, and none of the exceptions applied based on their complaint. Certainly, liability would not be established based on that. There still would be arguments to be made. But you cannot establish any, unless you show that the Court has jurisdiction to evaluate the application of that statute as applied to the plaintiffs in the case on the facts asserted, and that is the defect here with respect to both of the claims that they say give them statutory standing, the Wiretap Act and Stored Communications Act.

And I would just commend your Honor to read their complaint and read our briefs, because we make this abundantly clear. The water has been muddied a little bit here, but I think it really is very clear on those two points. And with those two issues, there's no standing for the Court to begin the secondary inquiry of thinking about those other fact questions.

I see why those fact questions have been raised by the plaintiffs, because it starts to get the Court thinking about those issues. But the two issues that I described, the failure to raise harm, causation issues and the lack of statutory standing, those resolve this case.

There are quite a number of arguments I can respond to with respect to the arguments that Mr. Strange and Mr. Grygiel made. They're all in our papers. If you're tiring, I can sit down, but if you are prepared to hear

them, I will continue.

THE COURT: Well, I'm prepared to hear them for a moment anyway. I think I gave two hours. If I gave more than two hours, forget it. But I can sit here for at least the two-hour stretch.

MR. RUBIN: Okay. The point I want to make is around, pointing to a couple of very important things in the complaint that I think are important to see. They're in the complaint. These aren't factual disputes. This is just facts in the complaint.

A lot of words were said by my, by opposing counsel around information about users that was sent along, personal information around users.

If you look at the complaint, and Mr. Grygiel, I believe, cited paragraph 98 and footnote 67 of the complaint. That part of the complaint is talking about and citing to Google's privacy policy. But there's no allegation in this case that the four named plaintiffs are Google accountholders, so they would never have provided any of that information to Google. And I don't want to speak for the other defendants, but I think it's fair to say that those allegations don't apply to them at all. And they can get up and correct me if that's wrong.

So there's just no allegation that that sort of information has been provided by anyone here. Sure, if you

have a Google account, you sign up, give your name and do all sorts of things. These, these plaintiffs do not allege to be Google accountholders, so the suggestion that they're browsing, this is limited browser information that's sent by their browsers and then to which the cookie goes along for the ride after it's placed is somehow commingled, finds no factual support whatsoever in the complaint and can't be credited.

The other point I want to make with respect to all of the complaint, all of the arguments they made is, they talk about a lot of the underlying violations of the statutes they believe occurred, but they came back with very little response on the financial arguments, rather, the harm arguments. The CFAA response by Mr. Grygiel I think is particularly instructive.

The loss issue or the damage issue there is required. There is no damage alleged in the complaint, period, so they have to have alleged $5,000 in damages, and they cannot have not done that. A benefit to someone else is not a loss within the meaning of the CFAA.

With respect to the Stored Communications Act, the facts that they have alleged in this case do create a situation of mutual exclusivity, so while some other case may have said, the fact that the Internet is packet switched means that there can be co-extensive application of these

statutes here, that does not apply on these facts and I think that's clear when you look at the statutes and look at what they've alleged.

And I will just say again what I said at the beginning. They are alleging under their new theory, this is in opposition, it was the one that they articulated here, that Google was an electronic communications service. If that is true in this context, 2701(c)(1) provides Google with authorization to access these materials. It had all of those other unwanted effects, too, but it has that issue.

And with respect to the California claims quickly, on the CCL, the computer crime claim, we have not seen the Path case because it wasn't in the papers. But Mr. Strange said it involved downloading an app that stole content from people's devices. There's no -- contacts from those devices.

There's no allegation in these cases that these cookies do anything like that. The allegations in this case are that their browsers sent get requests, that a cookie was placed and their browsers continued to send get requests, just as they did before. Those are the facts that they actually allege, if you look at the complaint.

And there's no allegation that would be actionable under California privacy, that mental health information or HIV information attached to someone's name

has been collected here.

And with respect to the unfair competition law, the substance of the prongs I've addressed in our papers, but Mr. Strange didn't have a response, I know, to the fact that there is a heightened statutory standing requirement and they can't pass it. There's no -- they have not lost money or property in this case.

So unless the Court has any questions?

THE COURT: Well, I'm not sure I can articulate my question, but I guess I just want to make -- I would be happy to know -- well, the plaintiff had some illustrations up there about the communications and I guess you agreed with them until it came to the brick wall?

MR. RUBIN: I say two things about their communications.

THE COURT: Right.

MR. RUBIN: It's all in their papers.

THE COURT: I think there were two, and the first one I thought -- well, that was the second one. Right.

I don't know if it is included anyplace and I want a copy of it, if this is an accurate representation of what's happening here. If it's not, I'd like you to tell me it's not, because I think it's important for me to have a basic understanding of the underlying receipt and transfer

of communications and information in order to be able to resolve this.

MR. RUBIN: Absolutely. I note in my first argument that there's no technique to the complaint and to the paragraphs in the complaint. And I personally, and I think it would help the Court, it would help to see what they're referring to in the complaint. And let me tell you what I see.

One, two, and three. Three is back and forth. That's all exactly right. That's this transaction. I mean, it's iframes' point is the specific point here. This is ads, right. This would be the user has Safari, asks -- I wouldn't articulate it this way. They said that's what they were talking about and they said they agreed. If there's a dispute around this, let me know.

Someone types in an URL at their browser. The browser sends it off to the Internet. There's actually an intermediate step here. Someone has to interpret what you are typing and route it. It gets to the Wall Street Journal. The Wall Street Journal says, I want to populate my page with some ads, probably a lot of other stuff, too: Facebook, share links and links from all over the place. Sends that information back to the browser. Some of it is the news content you want to get and some of it is placeholders for the services to insert their information.

So that's the first blue line. There would be a bunch of other blue lines going to services in reality. Goes to Google. Google says, okay, I'm going to send you back these ads. That's one.

Where I have an issue is with five, because five is not some independent thing that is now being enabled by a cookie and there's no support in their complaint for the suggestion that it is. The next time someone goes to a different website, if you type in NYTimes.CommunicationsAct, for example, this whole thing happens again.

THE COURT: One through four?

MR. RUBIN: One through four. One through four happens every time, and they have not cited it, they have not alleged it, and they can't allege it because it's just simply not right, that once a cookie is put on a browser, all of a sudden it enables new communication. All it does is enable the cookie to go along the next time that transaction goes.

But this is not, this is not in the complaint, that last part.

THE COURT: And the next page? Could I see the next page with brick wall? So that's another step.

MR. RUBIN: So often, often when services communicate back to, I guess the third step on the last page, often services will set cookies. That's often the way

cookies get set. That is the way the cookies get set. This is in their complaint as well. I don't know the page. They have a very lengthy background on how cookies get set, which is for the most part correct. In any event, we have to take it.

And so here the claim is Google set this one cookie, drt, and that there's a brick wall. Google did set a cookie. The brick wall is supposed to be Safari's default cookie block settings. Their allegation is, is that Safari's default cookie block settings actually allow cookies to be sent in any number of circumstances.

If you look at the materials in the request for judicial notice and this, sorry, and the complaint as a whole, you'll see that there's one method called this form post method that allowed a cookie to be set, but there are others. Clicking on a link allows it as well. There's all sorts of ways in this default setting.

So this is designed to create the impression that in its default setting, Safari was impregnable or blocked all cookies, but, in fact, that's not what happened.

It became relevant to the issues. It's in the complaint. This cookie isn't the cookie by which Google associates information, associates browsing information as received. This is something completely different. That other cookie got sent due to another quirk in the browser.

So I mean that's -- but this is all in the complaint. It's all detailed rather well, but in the RGN exhibits. But the point is, none of this the Court needs to wade into this morning because they have not alleged any harm, and on the two statutes that they assert that say would give them statutory standing, those communications go every time, and they go with a cookie or without a cookie. And this didn't enable anything. It didn't change how their browsers worked. Their browsers were working this way long before this whole incident came along and they're working the same way now.

They're sending get requests every time. We all do. It's just the way -- and this is in their complaint. This is how paragraph 41 explains it.

THE COURT: All right. Thank you.

MR. RUBIN: Thank you very much.

THE COURT: Again, I appreciate all of your time. I have to say that I generally use oral argument as a filter. When you give me too much information, I assume you're giving me the most information in oral argument and I appreciate your doing so.

I have a 4:00 o'clock proceeding. If plaintiff has any final thoughts, I'm happy to hear it before I send you on your way and I try to address the issues that you've presented.

MR. ROBERTSON: Your Honor, I don't want this to turn into a Ping-Pong match. I just want to tell you most of this -- we think all it is in paragraphs 85 to 95 of the complaint, and including the picture that we got from the Wall Street Journal saying where the brick wall comes in. So thank you for your time.

THE COURT: All right. Thank you. All right, counsel. Thank you again. I have to get out of my computer, so go home. Thank you very much.

(Counsel respond, "Thank you, your Honor.")

(Court recessed at 3:52 p.m.)

- - -